(2)

W3C® Technology and Society domain

Joint Workshop on Mobile Web Privacy

WAP Forum & World Wide Web Consortium

7-8 December 2000

Munich, Germany

Agenda
Minutes from workshop: Day 1, Day 2
Workshop Report and Summary
Position Papers
Participants
Background Materials
Call for Participation

Important dates
Registration deadline: *2 December 2000.*
Papers submission deadline: *6 November 2000.*

Workshop meter
On 1 December 2000: *45* registrations, *20* position papers expected, and *45* persons on the mailing list.

Pages created and maintained by Daniel J. Weitzner <djweitzner@w3.org> Mobile Web Privacy Workshop Co-Chair.

$Id: overview.html,v 1.5 20

Index of /P3P/mobile-privacy-ws/papers

Name	Last modified	Size	Description
Parent Directory	06-Apr-2004 22:31	-	
JPhoneEast.html	05-Dec-2000 15:27	2k	
arthurandersen.html	05-Dec-2000 15:54	52k	Wie sicher ist mobile >
avenuea.html	05-Dec-2000 05:18	13k	
dolev.html	05-Dec-2000 14:54	10k	CellularPersonalID
gundermann.html	04-Dec-2000 16:42	10k	Workshop on Mobile Web>
ibm.html	23-Nov-2000 02:05	12k	Mobile Web Privacy
ispe.html	05-Dec-2000 15:13	9k	IPSE_MunichWorkshop
karlstad.html	23-Nov-2000 01:41	11k	Privacy Enhancement in>
motorola.html	23-Nov-2000 01:53	3k	Joint Workshop on Mobi>
nextel.html	23-Nov-2000 01:37	23k	Privacy
nokia.html	23-Nov-2000 01:50	4k	Privacy for Location D>
siemens.html	23-Nov-2000 01:46	3k	R. Weber, Siemens Corp>
xypoint.html	23-Nov-2000 02:09	13k	Xypoint Position Paper
zks.html	23-Nov-2000 01:33	4k	The Difference Between>

Position paper: Privacy Enhancement in the Mobile Internet

Simone Fischer-Hübner, Helena Lindskog
Karlstad University
Computer Science Department
Sweden
http://www.cs.kau.se/~simone/
http://www.cs.kau.se/~helena/

Introduction:

Our Computer Security Research Group within the Computer Science Department at Karlstad University has recently started to work on the project "Enhancing Privacy for Web-based Services in wireline and wireless Networks". Within the project, we assess privacy threats and problems for the Mobile Web and work on privacy-enhancing technologies for protecting personal information. One major research issue is how the Composite Capability/Preference Profile (CC/PP) information can be protected by using CC/PP with P3P (Platform for Privacy Preferences) and how P3P can be enhanced.

Expectations on the final outputs of the workshop:

We expect that privacy problems and risks in the Mobile Web environment will be made clear. Besides, specific legal provisions to protect privacy in the mobile web needed in addition to existing general data protection legislation should be suggested. Privacy is increasingly becoming an international problem, because communication data often crosses state borders. An international harmonization of privacy legislation is necessary, but hardly achievable due to cultural differences (see also [Fischer-Hübner 2000]. The recent transatlantic debate about the adequacy of the Safe Harbor privacy principles in comparison with the EU data protection Directive has demonstrated the difficulty of harmonizing data protection regulations. For this reason and also because law is not an ultimate protection, it is important to protect and enforce privacy also by technology. Our main expectation on the final outputs of the workshop is therefore that privacy enhancing technologies for protecting the mobile web users should be discussed and suggested.

General perspective on privacy challenges raised by mobile Web services:

In the networked society, the individual's privacy is at risk. A side-effect of global wireline or wireless communication is that transactional data of the users can be collected at different sites (e.g., service provider site, server site, sites passing on messages) and can be used to create communication or consumer profiles.

WAP gateways receive, translate and forward all requests telling who requests what using what device and thus can easily create extensive personal user profiles.

Personal user data can also be accumulated at the origin server's site. Web or WAP server sites often ask for user- and user-side specific data to offer customized services or for market analysis purposes. Input parameters to a mobile context aware service can be the user identity, user location, device type and capabilities, user settings in the device, the user's previous behavior as well as PIM (personal information management) data.

The user identity can often be retrieved by the origin server behind the user's back, by using MSISDN number forwarding or user-id forwarding from the WAP gateway or an access server. Whether or not the user's actual identity can be retrieved depends on the type of subscription that the user has for the specific service. In most countries MSISDN forwarding to outside the operator's environment is forbidden by law, but it is sometimes possible to extend the operator's environment to include content providers. If user-id forwarding from other components in the network is not used, HTTP basic authentication (HTTP 401) or a simple web page logon procedure can be used to reveal the

user's identity.

Standard HTTP behavior is to have the browser name passed on with the request. However, in the mobile Internet world, passing on this information does not only tell the receiving application what application the user is running, as in the web case. From the browser name, the device type and version can usually be redrawn as well.

The Composite Capability/Preference Profiles (CC/PP) are proposed by W3C as a collection of capabilities and preferences associated with users and the user agents to access the World Wide Web. Particularly in wireless networks CC/PP is intended to provide information necessary to adapt the content and the content delivery mechanisms to best fit the capabilities and preferences of the users and their agents. However, the capabilities and preference information (CPI) contains detailed characteristics about the user's device, software, network and personal settings, which can be unique for a specific user with a specific device. Thus, the CPI can serve as a unique identifier and can, like a user-id, be used to trace a user's request activities at the origin server's site. CPI in combination with the user-id can tell what device, software or network a user is using. Such information can be misused for launching attacks against the user, if it gets into the wrong hands.

The User Agent Profile (UAProf) specification, which seeks interoperability with the CC/PP standard, also defines the user location as a reserved attribute. The user's location can be retrieved in two ways. Either by using GPS or similar integrated with the device, and then send the information with the request, or by having the application retrieve the user's position through the knowledge that the operator has based on radio base station information. Sending the position with the request can be done in several ways: by using the UAProf attribute, or a proprietary HTTP header.

Thus at the server site, different personal characteristics of users can be available, which could be used to trace their requests, habits, preferences and movements and to create user profiles. For context-aware services, extensive storage of user data is necessary. On the other hand, the user's privacy rights and interests have to be protected as well.

Our potential contributions:

1. Suggestion how CC/PP can be used with P3P:

   The CC/PP working group has already expressed the design goal that P3P is to be used as a management mechanism for the privacy of profiles. P3P by W3C is a protocol designed to inform Web users of the data-collection and data-use practices (P3P policy) of web-sites and to help users to reach a semi-automated agreement with web-sites with regard to the processing of an individual's personal data.
   P3P can be used to enhance the user's privacy by transmitting CPI (and possibly other other personal characteristics) only if there is an informed consent by the user about the origin server's site data collection and use practices (how and for what purpose CPI will be used, with whom data will be shared, how long the data will be retained).
   However, CC/PP cannot directly be combined with the P3P standard. With the CC/PP exchange protocol, a user uses a modified HTTP GET request which already carries the profile or profile difference, whereas according to the P3P standard it is first checked whether there is a sufficient match between a user's privacy preferences and the remote server's privacy policy before any personal data is transmitted.
   Thus, in order to use CC/PP with the P3P standard, the CC/PP exchange protocol should first use a GET request that carries a profile with only minimal information about device properties (such as screen size, voice/ graphic capabilities), to which a service would respond with a reference to a P3P policy. The user agent would then fetch the policy and compare it with the user's preferences to determine whether CPI should be transmitted. The user should have the possibility to choose the level of protection by defining privacy preferences for the whole CPI, or different preferences for CPI components and/or attributes.

2. How can P3P be combined with other security mechanisms to support basic requirements of the EU data protection Directive:

   Whereas P3P can implement informed consent, P3P alone does not support other basic provisions of the EU data

protection directive, such as purpose restriction (Art. 6b: legitimacy), necessity of data collection and processing (Art. 6c: adequacy) and the right of access (Art.12). Thus P3P alone is not a sufficient solution.

Within a former research project, a formal privacy model has been developed and implemented according the Generalized Framework of Access Control- Approach in the Linux system kernel [Fischer-Hübner / Ott 1998]. The privacy model was designed as a security model that can technically enforce legal privacy requirements such as purpose restriction and necessity of data processing. It is planned to adapt the privacy model implementation, so that it can be used in combination with third party monitoring and assurance to protect P3P data elements at the server's site, so that personal data elements are collected and processed only as far as necessary and only used for the specified purposes.

3. Encourage the discussions of privacy-enhanced system concepts to protect user identities at the WAP gateway site:

   The use of privacy-enhancing technologies such as for instance Mix nets for providing anonymity at the WAP gateway site should be examined. A Mix net introduced by D. Chaum [Chaum 1981] can realize unlinkability of sender and recipient and sender anonymity against the recipient. If a request would be send through a mix net to the gateway, the user identity could be hidden from the gateway.

References:

[Chaum 1981] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24 (2). 1981, pp. 84-88, http://world.std.com/~franl/crypto/chaum-acm-1981.html

[Fischer-Hübner/Ott 1998] Simone Fischer-Hübner, Amon Ott, "From a Formal Privacy Model to its Implementation", Proceedings of the 21st National Information Systems Security Conference, Arlington, VA, October 5-8, 1998

[Fischer-Hübner 2000] Simone Fischer-Hübner, "Privacy and Security at Risk in the Global Information Society", in: D.Thomas, B.Loader (Eds.): Cybercrime, Routledge, London and New York, 2000

Privacy Enhancement in the Mobile Internet

Simone Fischer-Hübner, Helena Lindskog
Karlstad University / Sweden
In cooperation with
Ericsson Infotech in Karlstad

Definition of Privacy:

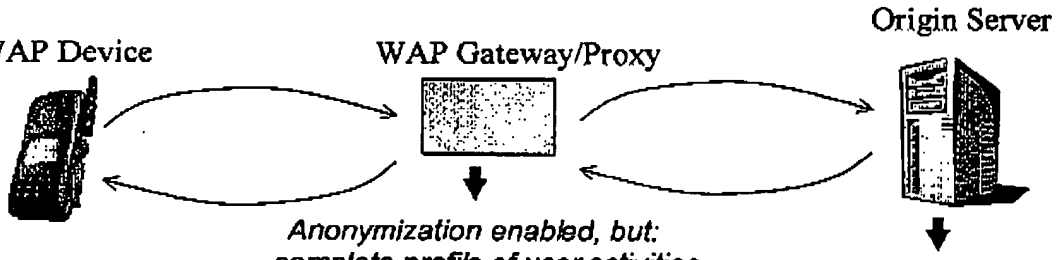
Alan Westin (Columbia University, 1967):

" the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"

Basic privacy principles:

- authorisation by law or consent
- necessity of data collection and processing
- purpose specification and purpose binding (there are no "non-sensitive" data)
- right of access / notification / objection
- supervision and sanctions
- adequate organisational and technical safeguards

Mobile Web Privacy Issues:



Anonymization enabled, but:
complete profile of user activities

- *user ID (if user logged on or if forwarded)*
- *CC/PP - CPI (device, software, network, pers. settings)*
- *- user location (UAProf reserved attribute)*

→ *Privacy is an international problem*

Problem of International Harmonisation of Privacy Legislation:

Is a common harmonised approach to privacy possible
due to cultural/ historical/ political differences ?

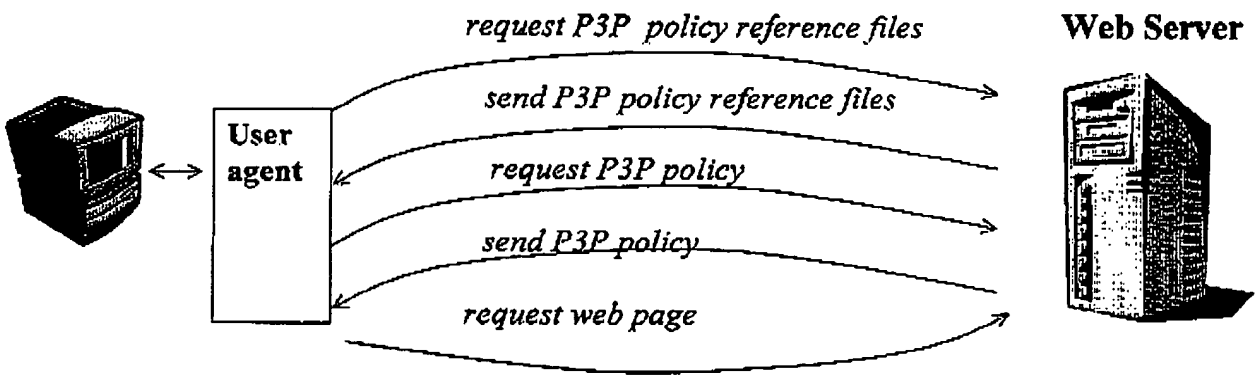
Example:

Europe:	vs.	USA:
- EU Data Protection Directive - EU Telecommunication Data Protection Directive		no omnibus privacy legislation, self-regulation in the private sector, no oversight authority

Safe Harbour Principles as a solution ?

Protection at Server site: Combining P3P and CC/PP

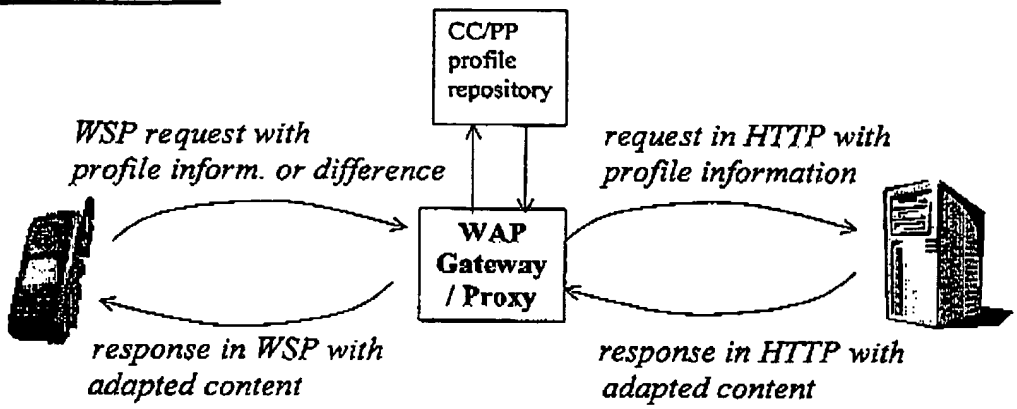
Platform for Privacy Preferences (P3P):



User agent has to:
- request P3P policy reference file
- request P3P policy
- match policy with user preferences
- accept/ reject/ inform/ warn

Indication to P3P policy reference file through:
- well-known location (/wc/p3p.xml)
- html link tag
- http header

CC / PP – WAP:


CC/PP profile repository
WSP request with profile inform. or difference
request in HTTP with profile information
WAP Gateway / Proxy
response in WSP with adapted content
response in HTTP with adapted content

Combining CC/PP and P3P:

- Initial request with minimal profile information (screen seize, voice, capabilities, graphic capabilities)
- Users should be able to define P3P preferences for whole CPI or for CPI components or attributes
- P3P categories for CPI: computer, preferences, location

P3P Enhancements:

P3P privacy problems:

Are users forced/pushed to give-up privacy ?

P3P alone does not fulfil the following EU-Directive requirements:

- Legitimacy (Art. 6b)
- Adequacy (Art. 6c)
- Right of Access (Art.12)
- Adequate level of protection for transborder data flow

Protection of P3P data at the Server site:

Formal Task-based Privacy Model + Third Party Assurance

A Formal Task-based Privacy Model:

∀ S : Subjects, O : Personal Data Objects :

Task-Authorisation:

current-task (S) ∈ authorised-tasks (S)

TP-Authorisation:

Current-TP (S) ∈ authorised-TP (current-task (S))

Necessity of data processing:

If S has x-access to O ⇒

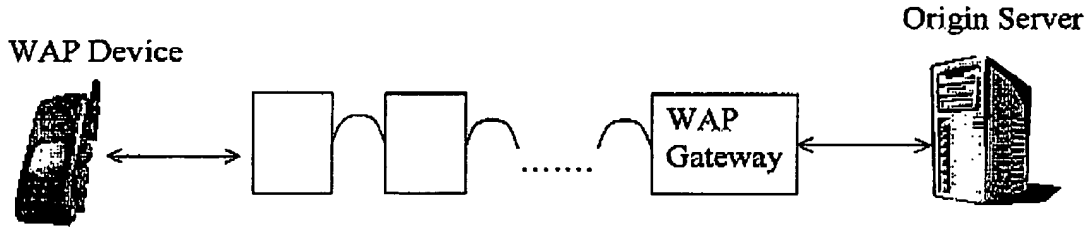
(current-task (S), class (O), current-TP (S), x) ∈ necessary-accesses

Purpose binding:

If S has x-access to O ⇒
purpose (current-task (S)) ∈ purposes (class (O)) ∨
(purpose (current-task (S)), O) ∈ consent

Protection at the WAP Gateway Site

Anonymizing Proxies or Mix net concepts
for protecting User Identities ?



ERICSSON

PATENT CASE PAGER 1 (5)

Upplagd (även fakturaansvarig om annan) - Prepared (also subject responsible if other)	Nr - No.	
EIN/L/I Helena Lindskog	EIN/L-01:0062	P14463
Delsnitt/Godk - Doc responsible/Approved / Kontr - Checked	Datum - Date	Rev / File
	2001-03-08	A / EINL:09

KOPIA (6)

1 TITLE OF THE INVENTION

Minimal Profile Conveyance - enhanced P3P for Mobile Internet.

2 INVENTOR

Helena Lindskog, Mikael Nilsson and Simone Fischer-Hübner.

3 TECHNICAL FIELD

Privacy in Mobile Internet.

4 STATE OF THE ART

In a very short time, the mobile Internet has grown into immense proportions. Its mechanisms allow users both to access the Internet services and other server-based applications from mobile devices, and make new services possible, such as location-based and context-aware applications. Today, WAP (Wireless Application Protocol) and iMode are the most frequently used technologies besides standard HTML over modified TCP/IP used in most Personal Digital Assistants (PDA). While mobile web services can be of great use, the privacy risks have to be considered, and appropriate data pro-tection and privacy safeguards must be ensured. It is necessary to prevent mobile Internet users to be under permanent surveillance and that the only possibility for them to protect their privacy is not to use the mobile services at all.

5 PROBLEM

The W3C P3P candidate recommendation specifies a protocol that provides an automated way for users to gain more control over the use of personal data on web sites they visit. P3P enables Web sites to express their privacy practices in a machine-readable XML format that can be retrieved automatically, interpreted easily and compared with the user's privacy preferences by user agents. Using this information, the user can make informed decisions on whether or not to submit a certain piece of personal information to the Web site.

In order to protect the user's right for informational self-determination, users should have control over the CPI of their devices, and determine themselves how far and to what extent they want to communicate profile information to other sites.

The CC/PP working group has expressed the design goal that the Platform for Privacy Preferences (P3P) is to be used as a management mechanism for the privacy of profiles. P3P can enhance the user's privacy by transmitting CPI (and possibly other personal characteristics, such as location data – unless already included as an CPI attribute) only if there is an informed consent by the user about the origin server's site data collection and use practices (how and for what purpose CPI will be used, with whom data will be shared, how long the data will be retained).

However, with the CC/PP exchange protocol, a user uses a modified WSP or HTTP GET request which already carries the profile information or profile difference,

Upprätt (även ärendeansvarig om annat) - Prepared (also subject responsible if other)	Nr - No.	
EIN/L/I Helena Lindskog	EIN/L-01:0082	
Delansv/Godk - Dep./subjrs/Approved / Kontr - Checked	Datum - Date / Rev	File
	2001-03-08 A	

whereas according to the P3P standard, it is first checked whether there is a sufficient match between a user's privacy preferences and the remote server's privacy policy before any personal data is transmitted.

6 SOLUTION

Thus, in order to use CC/PP with the P3P standard, it is first required that the user defines a minimal profile with only minimal CPI. This minimal profile should include only such CPI (such as for instance screen size, voice or graphic capabilities) that the user is ready to reveal even to sites with whom the user has not come to a P3P agreement so far. In the extreme case in which the user does not want to provide any information to possibly non-trustworthy sites, the user could define that the minimal profile be empty.

Thus, the minimal profile can be used

- for communication in the "safe-zone" before a P3P agreement;
- for accessing non-P3P enabled web sites or web sites that do not meet the user's P3P privacy preferences;
- and optionally for serving third party requests to the WAP Gateway for cached profiles (for instance, to generate content that will subsequently be pushed to the client device)

The following use case describes the steps of communication for the case where the user has defined a minimal profile and the P3P protocol is used to agree about the data collection and use of further CPI:

1. Upon opening a WSP session, the client conveys its minimal profile information using Profile and Profile-Diff headers within the WSP Connect request. The WAP Gateway caches the minimal profile for the lifetime of the session.
2. If the user wants to request content from a P3P enabled site, she first requests the site's P3P policy reference file by issuing a standard WSP request to the WAP Gateway. The WAP Gateway forwards the request via HTTP including the user's minimal CPI associated with the session. After having received the policy reference file, the user requests the privacy policy in the same manner. Thus, for the communication in the safe zone, only the minimal profile is forwarded by the WAP Gateway to the origin server.
3. The user agent compares the site's privacy policy with the user's preferences to determine whether further CPI should be transmitted. Users should have the possibility to choose the level of protection by defining privacy preferences for the whole CPI, or different preferences for CPI components and/or attributes.
4. If the user or her agent accepts the origin server site's privacy policy, there are different options of how further CPI can be transmitted to the origin server:

Upphovs (även namnteckning och namn) - Prepared (also subject responsible if other)	Nr - No.		
EIN/L/I Helena Lindskog	EIN/L-01:0082		
Granskad/Godk - Rev resp/Approved / Kontr - Checked	Datum - Date	Rev	File
	2001-03-08	A	

5. To augment the minimal profile, the client includes profile and/or profile-diff headers with each subsequent WSP request in that session as depicted in Figure 1. The WAP Gateway then overrides the cached minimal profile with the provided headers, when it generates an HTTP request.

6. The user sends a WSP session Resume message to the WAP Gateway containing profile and/or profile-diff headers with the new CPI and the WAP Gateway will update the cached CPI for that session, as shown in Figure 2.

Also, if the user agrees that certain CPI attributes (e.g., the user location) might be augmented by the WAP Gateway, the WSP requests or resume message should have a flag/attribute set that authorizes the WAP Gateway to add that information to the CPI.

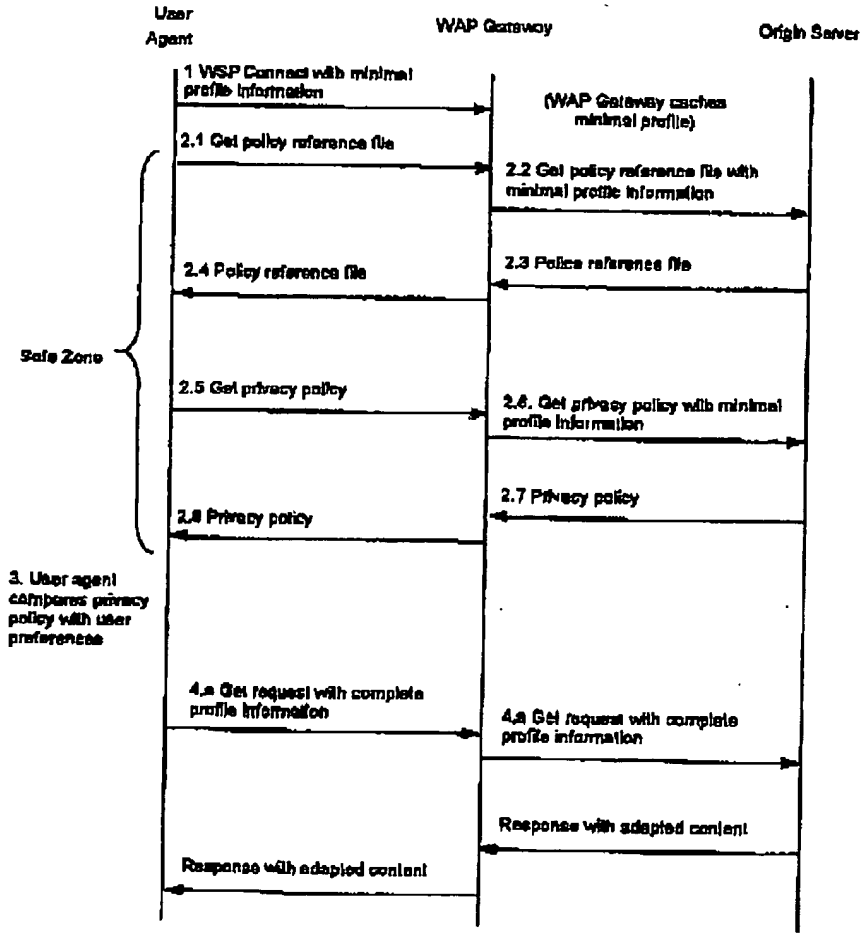


Figure 1: The complete CPI is conveyed with every WSP request issued after the P3P agreement

ERICSSON

PATENT C PAGER 4 (5)

Upprättad (även fakta/ansvarig om annan) - Prepared (also subject responsible if other)	Nr - No.
EIN/L/I Helena Lindskog	EIN/L-01:0082
Granskad/Godk - Doc responsible/Approved / Kontr - Checked	Datum - Date / Rev / File
	2001-03-08 A

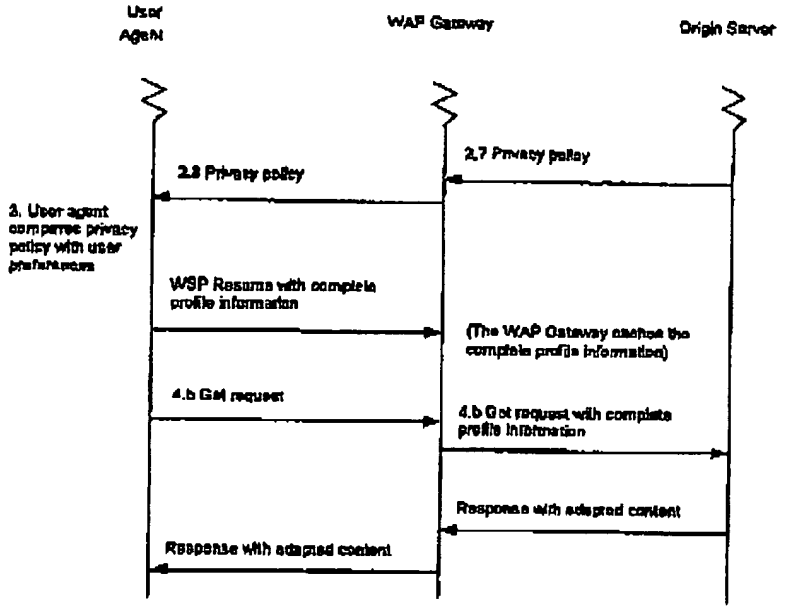


Figure 2: The complete CPI is sent with the WSP Resume after the P3P agreement

Upprättad (även telefonnummer och e-postadr) - Prepared (also subject responsible if other)	Nr - No.	
EIN/L/I Helena Lindskog	EIN/L-01:0082	
Dokansvarig/Godk - Doc responsible/approved / Kontr - Checked	Datum - Date / Rev	File
	2001-03-08 A	

Sending the complete profile information with each subsequent request has the advantage that the complete CPI profile of user device will not be cached in the WAP Gateway. However, in contrast to option 4.b, also CPI, and thus more data, has to be transferred with each request. Option 4.b can only be used if one privacy policy is valid for an entire Web site.

7 BENEFITS FOR ERICSSON

The need for a privacy proxy and a corresponding terminal solution is urgent. People might refuse to use the mobile Internet if privacy is neglected. Failing to provide such an implementation might cause reduced sales of mobile terminals. We will also have a chance to develop and sell serverside solutions.

8 DEVELOPMENT PROJECT

These ideas were developed within a research project, consisting of both Ericsson and university personel.

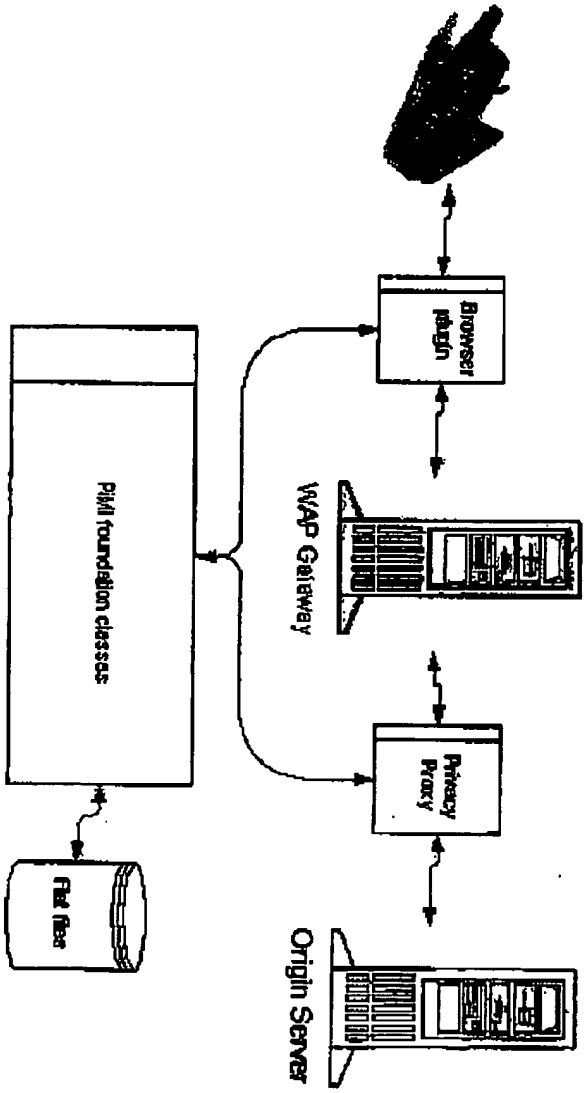
9 LAST POSSIBLE FILING DATE

ASAP.

10 OTHER COMMENTS

Read and Understood by:..... Date:.....

Read and Understood by:..... Date:.....



print.jpg (617x304x16M jpeg)

ERICSSON

Ingalill Ohlsson 08-585 32020

Date: June 15, 2001 | Our Reference: P14463US | Diarie no.: PUIA:01: 10106

34647-438USPT

(7)

Via fax, original by mail
Per Ljungqvist
Mikael Nilsson
Helena Lindskog
Simone Fischer-Hübner

Brian Walker
Jenkens & Gilchrist
1445 Ross Avenue
Suite 3200
Dallas, TX 75202-2799
USA

POSSIBLE NEW U.S. PATENT APPLICATION

Our Reference:	P14463
Title:	Minimal Profile Conveyance
Beneficiary Owner:	Patent Unit Internet Applications

Enclosures

1. General instructions and Checklist
2. Invention Disclosure

We would like you to start drafting a patent application based on this invention after you have contacted the patent engineer. After approval from the patent engineer of the final draft please file a patent application.

Target date for filing an application: August 31, 2001

A patent application based on this invention must be filed before November 30, 2001.

Applicant:	**Telefonaktiebolaget L M Ericsson (publ)** **SE-126 25 STOCKHOLM** **SWEDEN**	
Inventor(s):	NILSSON; Mikael, Hagagatan 14B, SE-652 20 Karlstad, SWEDEN Phone: +46 54 294 122	Citizenship: Swedish
	LINDSKOG; Helena, Tomtebogatan 6 SE-655 63 Karlstad, SWEDEN Phone: +46 54 294 224	Swedish
	FISCHER-HÜBNER; Simone Gitarrgatan 96 SE-656 36 Karlstad, SWEDEN	German

ERICSSON

Ingalill Ohlsson 08-585 32020

Date: June 15, 2001 | Our Reference: P14463US | Claim no.: PUIA:01: 10106

Patent Engineer: Hjalmar Emillon,
ERICSSON INTERNET APPLICATIONS AB
Patent Unit Internet Applications
Box 48
SE-164 93 Kista
SWEDEN
Phone: +46 8 585 30281 Fax: +46 8 757 2770

Assistant: Ingalill Ohlsson
Phone: +46 8 585 32020

Please send all correspondence (incl. invoices) to the the address below and do not forget to quote our reference P14463US:

ERICSSON INTERNET APPLICATIONS AB
Attention: Ingalill Ohlsson
Patent Unit Internet Applications
Box 48
SE-164 93 Kista
SWEDEN

Please confirm safe receipt of this letter.

Yours faithYours faithfully,

ERICSSON INTERNET APPLICATIONS AB
Patent Unit Internet Applications

Ingalill Ohlsson
Patent Assistant

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

1445 ROSS AVENUE
SUITE 3200
DALLAS, TEXAS 75202

(214) 855-4500
FACSIMILE (214) 855-4300

www.jenkens.com

AUSTIN, TEXAS
CHICAGO, ILLINOIS
HOUSTON, TEXAS
LOS ANGELES, CALIFORNIA
NEW YORK, NEW YORK
SAN ANTONIO, TEXAS
WASHINGTON, D.C.

From the desk of:
Brian D. Walker
(214) 855-4706

RECIPIENT	COMPANY	FAX NO.	PHONE NO.
Hjalmar Emillon	Ericsson Internet Applications AB	+46 8 757 2770	+46 8 585 30281

• MESSAGE •

Please see attached letter.

Time: 12:59 PM **Date:** June 15, 2001 **Employee No.:** 2612 **Billing #:**34647-438USPT **Total Pages (+ cover):** 2

Jenkens & Gilchrist
A PROFESSIONAL CORPORATION

1445 Ross Avenue
Suite 3200
Dallas, Texas 75202

(214) 855-4500
Facsimile (214) 855-4300

www.jenkens.com

Austin, Texas (512) 499-3800
Chicago, Illinois (312) 425-3900
Houston, Texas (713) 951-3300
Los Angeles, California (310) 820-8800
New York, New York (212) 704-6000
San Antonio, Texas (210) 246-5000
Washington, D.C. (202) 326-1500

Brian D. Walker
(214) 855-4706
bwalker@jenkens.com

June 15, 2001

CONFIRMATION VIA FACSIMILE

Purchase Order No. IEP0684209
Patent Order No. P14463I
Ericsson Reference No. P14463US

Ms. Ingalill Ohlsson
Ericsson Internet Applications AB
Patent Unit Internet Applications
Box 48
SE-164 93 Kista
SWEDEN

Title: Minimal Profile Conveyance

Dear Ingalill:

This letter is an acknowledgment of your Patent Order. The following information should be referred to in the future:

J&G Responsible Attorney:	Brian D. Walker
J&G Associate Attorney	Brian D. Walker
J&G Reference No.:	34647-00438USPT
Disclosure Received:	June 15, 2001
Target Preparation:	July 31, 2001
Target Filing:	August 31, 2001

If you have any other questions regarding the above, please call the J&G contact identified above.

Very truly yours,

Brian D. Walker

BDW/meo

cc: Hjalmar Emillon

Dallas2 791242 v 1, 34647.00001

n J. Williams Approval _____

Intellectual Property Practice Group *New Patent Matter Data Form*			
Matter Name	Minimal Profile Conveyance		
Client Data	**Client Name:**	Ericsson Radio Systems AB - BMOA	
	Client Business Unit:	I - Internet Applications	
	Client Regional Office:	BR-Kista	
	Purchase Order #:	IEP0684209	
	Patent Order #:	P14463I	
	Client Reference #:	P14463US	
	Client Legal Contact (Atty/Engr.)	Hjalmar Emillon	
	Client Business Contact (Pat. Asst)	Ingalill Ohlsson	
	Technology Type:		
	Related Product:		
J&G Data	**Proposed Docket/Matter No.**	34647-00438USPT	
	J&G Office File Location	DA	
	Attorney Information	**Timekeeper #**	**Name**
	Biling Attorney	02612	Brian D. Walker
	Responsible Attorney	02612	Brian D. Walker
	Associate Attorney	02612	Brian D. Walker
	Paralegal		
Docket Codes	**Status/Substatus**	120	
	Disclosure Received Date (DSC)	June 15, 2001	
	Target Preparation Date (DIR)	July 31, 2001	
	Target Filing Date (FAP)	August 31, 2001	
	Foreign Filing		
Inventors	**Number of Inventors:**	3	
	Inventor Names:	Mikael Nilsson	
		Helena Lindskog	
		Simone Fischer-Hübner	

Date: June 15, 2001 Signature: Marcy Overstreet Marcy Overstreet